ISSN 1995-0802, Lobachevskii Journal of Mathematics, 2018, Vol. 39, No. 7, pp. 1039–1045. © Pleiades Publishing, Ltd., 2018.

Attacking Quantum Hashing. Protocols and Their Cryptanalysis

M. T. Ziatdinov[*]

(Submitted by F. M. Ablayev)

Kazan (Volga region) Federal University, ul. Kremlevskaya 18, Kazan, Tatarstan, 420008 Russia

Received December 6, 2017

Abstract—Quantum hash functions are similar to classical (cryptographic) hash functions and their security is guaranteed by physical laws. However, security of a primitive does not automatically mean that protocols based on this primitive are secure. We propose protocols based on quantum hash function and assess their security using Holevo entropy and recently introduced notion of quantum information cost.

DOI: 10.1134/S1995080218070211

Keywords and phrases: *Quantum hash functions, Holevo entropy, quantum information cost.*

1. INTRODUCTION

Quantum hash functions are similar to classical (cryptographic) hash functions and their security is guaranteed by physical laws. However, security of a primitive does not automatically mean that protocols that use this primitive are secure. We propose two protocols based on quantum hash functions and assess their security. We use Holevo entropy and recently introduced notion of quantum information complexity.

Quantum hash functions used in this paper are good candidates for experimental implementation. They use a small number of qubits and have an easy verifying procedure. The problem is that such quantum hash functions require maximum entanglement.

Quantum hash functions were first implicitly introduced in [1] as quantum fingerprinting. Then Gavirsky and Ito [2] noticed that quantum fingerprinting can be used as cryptoprimitive.

[3] gave a definition and construction of non-binary quantum hash functions. Ziatdinov [4] showed how to generalize quantum hashing to arbitrary finite groups. Recently, Vasiliev [5] showed how quantum hash functions are connected with ϵ-biased sets. Ziatdinov [6] introduced keyed quantum hash functions (QMAC).

Quantum hash functions map a classical message into a Hilbert space. Such space should be as small as possible, so eavesdropper can't read a lot of information about the classical message (this is guaranteed by physical laws as Holevo—Nayak's theorem states). But images of different messages should be as far apart as possible, so the recipient can check that hash differ or not with high probability. We measure this distance using an absolute value of scalar product of hashes of different messages. More detailed introduction to quantum hash functions can be found in Ablayev et al. [7].

The rest of this article is organized as follows. Next section contains necessary definitions. Section 3 contains definitions of analyzed protocols. Section 4 contains analysis of security of protocols based on quantum information cost. Section 5 is devoted to computing Holevo entropy of quantum hash.

[*] E-mail: gltronred@gmail.com